

# EXHIBIT 1

Magistrate Judge Michelle L. Peterson

CERTIFIED TRUE COPY  
ATTEST: WILLIAM M. McCOOL  
Clerk, U.S. District Court  
Western District of Washington

By Emily Nero  
Deputy Clerk

UNITED STATES DISTRICT COURT FOR THE  
WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff

v.

DENYS IARMAK,  
aka "Denys Olegovich Iarmak,"  
aka "Denis Jarmak,"  
aka "Denys Olehovych Yarmak,"  
aka "gaktus,"  
aka "gaktus01,"  
aka "denis.jarmak,"

Defendant.

NO. **19-564**

COMPLAINT

Title 18, United States Code, Sections 371,  
1029(a)(3), (b)(1), (c)(1)(A), and 2.

*Filed Under Seal*

BEFORE the Honorable Michelle L. Peterson, United States Magistrate Judge,  
United States Courthouse, Seattle, Washington.

The undersigned complainant being duly sworn states:

**COUNT 1**

**(Conspiracy to Commit Computer Fraud and Abuse)**

**I. OFFENSE**

1. Beginning at a time unknown, but no later than September 2015, and  
continuing through on or about November 20, 2019, within the Western District of

1 Washington, and elsewhere, the defendant, DENYS IARMAK, and others known and  
2 unknown, did knowingly and willfully combine, conspire, confederate and agree together  
3 to commit offenses against the United States, to wit:

4 a. to knowingly and with intent to defraud, access a protected computer  
5 without authorization and exceed authorized access to a protected computer, and by  
6 means of such conduct further the intended fraud and obtain anything of value exceeding  
7 \$5,000.00 in any 1-year period, in violation of Title 18, United States Code, Sections  
8 1030(a)(4) and (c)(3)(A); and

9 b. to knowingly cause the transmission of a program, information,  
10 code, and command, and as a result of such conduct, intentionally cause damage without  
11 authorization to a protected computer, and cause loss to one or more persons during a 1-  
12 year period aggregating at least \$5,000.00 in value and damage affecting 10 or more  
13 protected computers during a 1-year period, in violation of Title 18, United States Code,  
14 Sections 1030(a)(5)(A) and (c)(4)(B)(i).

## 15 **II. OBJECTIVES OF THE CONSPIRACY**

16 2. The objectives of the conspiracy included hacking into protected computer  
17 networks using malware designed to provide the conspirators with unauthorized access  
18 to, and control of, victim computer systems. The objectives of the conspiracy further  
19 included conducting surveillance of victim computer networks and installing additional  
20 malware on the victim computer networks for the purposes of establishing persistence,  
21 and stealing payment card track data, financial information, and proprietary, private, and  
22 non-public information, with the intention of using and selling such stolen items, either  
23 directly or indirectly, for financial gain. The objectives of the conspiracy further  
24 included installing malware that would integrate victim computers into a botnet that  
25 allowed the conspiracy to control, alter, and damage compromised computers.

## 26 **III. MANNER AND MEANS OF THE CONSPIRACY**

27 3. The manner and means used to accomplish the conspiracy included the  
28 following:

1           a.     The conspiracy developed and employed various malware designed  
2 to infiltrate, compromise, and gain control of the computer systems of victim companies  
3 operating in the United States and elsewhere, including within the Western District of  
4 Washington. The conspiracy established and operated an infrastructure of servers,  
5 located in various countries, through which members coordinated activity to further the  
6 scheme. This infrastructure included, but was not limited to, the use of command and  
7 control servers, accessed through custom botnet control panels, that communicated with  
8 and controlled compromised computer systems of victim companies.

9           b.     The conspiracy targeted victims in the Western District of  
10 Washington, and elsewhere, using, among other things, phishing techniques to distribute  
11 malware designed to gain unauthorized access to, take control of, and exfiltrate data from  
12 the computer systems of various businesses. The conspiracy typically initiated its attacks  
13 by delivering, directly and through intermediaries, a phishing email with an attached  
14 malicious file, using wires in interstate and foreign commerce, to an employee of the  
15 targeted victim company. The attached malicious file was embedded malware. The  
16 phishing email, through false representations and pretenses, fraudulently induced the  
17 recipient to open the attachment and click on the file to unwittingly activate the malware.

18           c.     If the recipient activated the malware, the computer on which it was  
19 opened would become infected and connect to one or more command and control servers  
20 controlled by conspiracy to report details of the newly infected computer and download  
21 additional malware. The command and control infrastructure relied upon various servers  
22 in multiple countries, including, but not limited to, the United States.

23           d.     The conspiracy typically would install additional malware to  
24 establish remote control of the victim computer. Once a victim's computer was  
25 compromised, the conspiracy would incorporate the compromised machine or "bot" into  
26 a botnet.

27           e.     The conspiracy used its access to the victim's computer network and  
28 information gleaned from surveillance of the victim's computer systems to install

1 additional malware designed to target and extract particular information and property of  
2 value, including payment card data and proprietary and non-public information.

3 f. The conspiracy frequently targeted payment cards used at the victim  
4 companies by customers making legitimate point-of-sale (POS) purchases. In those  
5 cases, the conspiracy configured malware to extract, copy, and compile the payment card  
6 data, and then to transmit the data from the victim computer systems to servers controlled  
7 by conspiracy.

8 g. The conspiracy then monetized that stolen payment card data by,  
9 among other things, offering the payment card data for sale on various websites dedicated  
10 to such carding activity.

#### 11 **IV. OVERT ACTS**

12 4. In furtherance of the conspiracy, and to achieve the objects thereof, the  
13 defendants, and others known and unknown, did commit and cause to be committed, the  
14 following overt acts, among others, in the Western District of Washington and elsewhere:

15 a. On or about August 8, 2016, the conspiracy sent multiple phishing  
16 emails, containing a file embedded with malware, to an employee of the Emerald Queen  
17 Hotel and Casino (EQC), a federally recognized Native American Tribe with locations in  
18 Pierce County, within the Western District of Washington.

19 b. Between on or about March 24, 2017, and April 18, 2017, the  
20 conspiracy harvested payment card data from point-of-sale devices from Chipotle  
21 Mexican Grill, including dozens of locations in the Western District of Washington.

22 c. On or about April 28, 2017, DENYS IARMAK communicated with  
23 another member of the conspiracy in furtherance of the hacking activity, including  
24 discussing the creation and use of phishing emails.

25 d. On or about on July 24, 2017, DENYS IARMAK and another  
26 member of the conspiracy discussed information stolen from a victim company.

1 e. On or about October 27, 2017, DENYS IARMAK and another  
2 member of the conspiracy discussed information about the compromised computer  
3 system of a victim company.

4 All in violation of Title 18, United States Code, Section 371.

5 **COUNT 2**

6 **(Access Device Fraud)**

7 5. The allegations set forth in above paragraphs are re-alleged and  
8 incorporated as if fully set forth herein.

9 6. Beginning at a time unknown, and continuing through on or about  
10 November 20, 2019, within the Western District of Washington, and elsewhere, the  
11 defendant, DENYS IARMAK, and others known and unknown, knowingly and with  
12 intent to defraud, possessed fifteen or more counterfeit and unauthorized access devices,  
13 namely, payment card data, account numbers, and other means of account access that can  
14 be used, alone and in conjunction with another access device, to obtain money, goods,  
15 services, and any other thing of value, and that can be used to initiate a transfer of funds,  
16 and aided and abetted such conduct; said activity affecting interstate and foreign  
17 commerce.

18 All in violation of Title 18, United States Code, Sections 1029(a)(3), 1029(b)(1),  
19 1029(c)(1)(A), and 2.

20  
21 And the complainant states that this Complaint is based on the following  
22 information:

23 I, Briana L. Neumiller, being first duly sworn on oath, depose and say:

24 **I. INTRODUCTION AND AGENT BACKGROUND**

25 7. I am a Special Agent with the Federal Bureau of Investigation (FBI), and  
26 have been since 2009. I am assigned to the Cyber squad where I investigate computer  
27 intrusions. My experience as an FBI Agent includes the investigation of cases involving  
28 the use of computers and the Internet to commit crimes. I have received training and

1 gained experience in interviewing and interrogation techniques, arrest procedures, search  
2 warrant applications, the execution of searches and seizures, Cybercrimes, computer  
3 evidence identification, computer evidence seizure and processing, and various other  
4 criminal laws and procedures. I have participated personally in the execution of search  
5 warrants involving the search and seizure of computer equipment.

6 8. As set forth herein, I submit that probable cause exists to establish that the  
7 defendant, DENYS IARMAK, knowingly and intentionally participated in a scheme to  
8 hack the protected computer networks of various victim entities and steal payment card  
9 data and information, which constitute unauthorized "access devices," in violation of  
10 federal law, to include Conspiracy to Commit Computer Fraud and Abuse, in violation of  
11 Title 18, United States Code, Section 371, and Access Device Fraud, in violation of Title  
12 18, United States Code, Sections 1029(a)(3), 1029(b)(1), 1029(c)(1)(A), and 2.  
13 Accordingly, I seek the issuance of an arrest warrant for IARMAK.

14 9. The facts set forth in this Affidavit are based on my own personal  
15 knowledge; knowledge obtained from other individuals during my participation in this  
16 investigation, including other law enforcement personnel and computer scientists; review  
17 of documents and records related to this investigation; communications with others who  
18 have personal knowledge of the events and circumstances described herein; and  
19 information gained through my training and experience. Because this Affidavit is  
20 submitted for the limited purpose, it does not set forth each and every fact that I or others  
21 have learned during the course of this investigation.

## 22 II. SUMMARY OF PROBABLE CAUSE

### 23 A. Background

24 10. U.S. authorities are investigating a transnational cybercriminal group  
25 engaged in a hacking and fraud scheme. Since at least September 2015, and continuing  
26 to the present, the group has attacked the protected computer networks of hundreds of  
27 businesses with the goal of infecting computer systems with malicious software (or,  
28 "malware") that allows the group to access and steal non-public information, such as



1 customer payment card data. Based on the initial estimates, this hacking scheme has  
2 stolen tens of millions of payment card numbers and has caused over 100 million dollars  
3 (U.S.) in losses to U.S. financial institutions and companies.

4 11. The hacking group generally, but not exclusively, targeted computer  
5 systems of businesses, primarily in the restaurant, gaming, and hospitality industries,  
6 including numerous confirmed victims located in the Western District of Washington.  
7 For instance, confirmed victims of the hacking group who have publically acknowledged  
8 being attacked include numerous restaurant chains, such as Chipotle Mexican Grill,  
9 including multiple store locations within the Western Washington. For example, between  
10 approximately March 24, 2017, and April 18, 2017, the group, having successfully  
11 breached the protected systems of numerous Chipotle restaurant locations, harvested  
12 payment card data from point-of-sale devices, including dozens of locations in the  
13 Western District of Washington.

14 12. The group also targeted the Emerald Queen Hotel and Casino (EQC), a  
15 hotel and casino owned and operated by a federally recognized Native American Tribe  
16 with locations in Pierce County, within the Western District of Washington. For  
17 instance, on or about August 8, 2016, the group, either directly or through intermediaries,  
18 sent multiple phishing emails, containing a file embedded with malware, to an employee  
19 of EQC.

20 13. Credit cards compromised through the group's prolific hacking activity  
21 affected accounts held at dozens of federally insured financial institutions and credit  
22 unions, including, among others, BECU, a credit union headquartered in the Western  
23 District of Washington. For example, on or about March 10, 2017, stolen card data  
24 related to accounts held at BECU, compromised through the computer network intrusion  
25 of a confirmed victim of this hacking group, was used to make unauthorized purchases at  
26 a merchant in Puyallup, Washington.



### The Hacking Group's Attack Methodology

14. The hacking group generally has targeted restaurants, hotels, and other businesses that engage in high volumes of point-of-sale payment card transactions. Generally, the hacking group attacks victim companies with phishing<sup>1</sup> emails that have attachments that either contain malware or link to malware. The phishing campaign will often involve a call to the recipient of a phishing email and the use of social engineering techniques to encourage the recipient to open the attachment and activate the group's malware.

15. For example, as part of a phishing campaign, a member or affiliate of the hacking group may call a hotel's customer service representative under the pretense of being a customer who wants to make a reservation. The caller will claim falsely that the details of the reservation request can be found in a file attached to an email previously sent by the caller. If the employee opens the attachment and activates the embedded malware, the computer on which it was opened will become infected and connect to the hacking group's command and control servers to report details of the newly infected computer and to download additional malware. The additional malware will run automatically and will connect to additional servers used by the scheme to establish remote control of the infected computer.

16. After gaining access to a victim's computer, the hacking group will deploy a wide variety of malware tools to conduct surveillance, control infected computers, and steal data. One of the hacking group's primary goals is to target point-of-sale systems

---

<sup>1</sup> Phishing is a technique in which the perpetrators use email messages and/or fake websites to trick people into providing information, such as network credentials (e.g., user names and passwords) that may later be used to gain access to the victim's systems. Phishing often utilizes social engineering techniques similar to traditional con-artist techniques in order to trick victims into believing they are providing their information to a trusted vendor or other acquaintance. Phishing emails are also often used to trick a victim into clicking on documents or links that contain malicious software that will compromise the victim's computer system.

1 that process high volumes of payment card transactions. Once the hacking group locates  
2 a point-of-sale system, it will use malware to capture and steal payment card data. The  
3 stolen data will then be sold on various criminal underground forums or through private  
4 sales.

5 17. The hacking group remains extremely active. The hacking group continues  
6 to launch extensive phishing attacks and steal point-of-sale information from businesses,  
7 such as fast food restaurants, that process a large volume of point-of-sale transactions.  
8 Additional phishing campaigns also indicate that the hacking group has expanded its  
9 reach, and is now attacking victims such as law firms and other service providers with  
10 access to customer lists or confidential financial information.

#### 11 **The Hacking Group's Use of a Virtual Work Environment**

12 18. The hacking group does not have a central office or work location. Instead,  
13 the hacking group uses a distributed work force that relies on a secure, virtual work  
14 environment to coordinate its illegal activity. This virtual work environment allows  
15 members in different cities and countries to remotely attack, access, and control victim  
16 computers in an organized fashion. This virtual work environment also allows the  
17 hacking group to tightly control who can access the work environment, thereby  
18 protecting the group's illegal activity.

19 19. One component of the virtual work environment is an elaborate network of  
20 servers located throughout the world that the hacking group uses as part of its command  
21 and control infrastructure. U.S. authorities have identified and examined a number of  
22 these command and control servers. This examination revealed that the servers are used  
23 to host control panels that allow the hacking group to remotely access and control  
24 compromised victim computers. Log data and intercepted communications demonstrated  
25 that members of the hacking group routinely access the control panels from their  
26 residences.

27 20. Another component of the virtual work environment is a number of  
28 communication servers located throughout the world that the hacking group uses to

1 facilitate the malware scheme. U.S. authorities have identified and examined a number  
2 of these servers. This examination demonstrated that the servers provide the hacking  
3 group with both secure channels of communication and virtual platforms on which they  
4 coordinate their attacks against victim companies even though each member is working  
5 from a remote location. For example, in approximately August 2017, foreign law  
6 enforcement provided U.S. authorities with a forensic image of a physical server used by  
7 the hacking group (hereinafter, "Server-1"). Analysis of the image showed that Server-1  
8 contained numerous virtual communication servers, including a private Jabber server that  
9 permitted members of the hacking group to have encrypted communications about their  
10 illegal activity. Jabber is an instant messaging service that allows members to send  
11 encrypted communications through a public or private server. In order to have an  
12 account within a private Jabber server, an administrator of the server must create an  
13 account for the user.

14 21. Examination of the hacking group's Jabber communications has allowed  
15 U.S. authorities to identify many members of the hacking group and their roles in the  
16 illegal enterprise. Although members of the hacking group generally used aliases and  
17 concealed their true names from each other, members regularly provided identifying  
18 information in Jabber communications with certain high-level members of the group to  
19 receive payment for their participation in the scheme. This information included  
20 information such as true names, addresses, bank account information, and information to  
21 receive digital currency or money order transfers.

22 22. Server-1 also contained virtual HipChat servers. HipChat is a group chat,  
23 instant messaging, and file-sharing program. Examination of the HipChat servers  
24 showed that the hacking group used HipChat to coordinate their efforts to breach the  
25 network securities of victim companies, to share stolen data such as payment card  
26 information, and to interview and recruit new members.

27 23. Through this investigation, which has included review of evidence obtained  
28 from foreign authorities, U.S. authorities obtained and examined a forensic image of

1 another physical server used by hacking group (hereinafter, "Server-2") in approximately  
2 November 2017. Like Server-1, Server-2 contained numerous virtual communication  
3 servers used to facilitate the malware scheme. Both Server-1 and Server-2 contained  
4 virtual JIRA servers. JIRA is a project management and issue-tracking program  
5 commonly used by software development teams. JIRA allows team members to create  
6 "projects" containing posted "issues" under which other team members can make  
7 comments and share data. This feature thereby facilitates collaboration between team  
8 members who may be working from different locations or during different hours.

9       24. Examination of Server-1 and Server-2 revealed that members of the  
10 hacking group used the JIRA servers to collaborate on their efforts to breach and steal  
11 data from victim companies. Often, hacking group members would create "issues" in  
12 JIRA with names that referenced a particular victim. Under each JIRA "issue", members  
13 would track their progress breaching the victim's security, upload data stolen from the  
14 victim, and provide guidance to each other. The JIRA servers logged activity related to  
15 an "issue" and tracked a variety of information including the user who created the  
16 "issue", users who commented under or uploaded files under the "issue", and users who  
17 otherwise had access to the "issue". This information has allowed investigators to link  
18 members to attacks against specific victims.

19       25. The hacking group's Jabber, HipChat, and JIRA communications confirm  
20 that the group's virtual work environment allowed the members of the group to work  
21 together closely even though the members were working from computers at their  
22 residences or from their mobile devices. In numerous conversations, members of the  
23 hacking group made reference to working at home or the need to go offline in order to  
24 run domestic errands such as going to the doctor's office. Notably, members of the  
25 hacking group were required to work late at night in order carry out malicious activity,  
26 such as sending phishing emails, during the business hours of victim companies who  
27 were located several time zones away.  
28

**Examination of Devices Belonging to Members of the Hacking Group**

26. The U.S. authorities' examination of devices belonging to individual members of the hacking group indicates that members of the hacking group keep extensive evidence of their illegal activity on their personal computers and mobile devices, including data that is exchanged through the hacking group's virtual work environment. For example, U.S. authorities examined a laptop seized by foreign authorities from the home of a member of the hacking group. The laptop contained many of the malware tools used by the hacking group in addition to credentials to remotely access the hacking group's servers. One of the malware tools was used over 1,200 times over the course of a 16-month period. Forensic examination of communications on the laptop indicate that the owner of the laptop was largely working from home when he developed phishing emails, attempted to breach victim computer systems, and stole data from compromised computers. In addition, the laptop had numerous folders, each dedicated to a specific victim, which contained data stolen from that victim. This stolen data included addresses for internal victim servers, login credentials (user name and password) for victim servers, tax information, customer order information, and other non-public information. Most notably, the laptop contained a variety of stolen financial information, including stolen credentials that could be used to access a victim's online bank accounts and over 4,000 unique payment card numbers. The laptop also contained extensive communications with dozens of members of the hacking group, including over 80,000 Jabber messages. In certain of these communications, the user of the laptop requested money order transfers in return for work performed on behalf of the hacking group.

27. Through this investigation, U.S. authorities also examined a laptop taken from a different member of the hacking group while he was on vacation in a foreign country. As with the first laptop, the second laptop contained extensive evidence of the malware scheme and information exchanged through the hacking group's virtual workspace. For example, the second laptop contained malware tools, credentials to



1 access the hacking group's servers, data stolen from victims, and over 4,000 payment  
2 card numbers. The laptop also contained over 85,000 Jabber communications with other  
3 members of the hacking group in which the owner of the laptop discussed his efforts to  
4 breach victims' networks, shared stolen data, and requested payment in digital currency  
5 for his work. Notably, the Jabber communications indicate that the hacking group was  
6 using a wide-variety of digital currency services or exchanges including, but not limited  
7 to, Binance, Electrum, EXMO.com, and Monero.

8 28. U.S. authorities have obtained evidence that members of the hacking group  
9 also use mobile devices to facilitate the malware scheme. In addition to private Jabber,  
10 HipChat, and JIRA servers, the hacking group uses a variety of other encrypted  
11 communication services such as Mumble, Telegram, Threema and Viber. U.S.  
12 authorities have gathered evidence that members of the hacking scheme access these  
13 communication services from their mobile devices. For example, pursuant to a mutual  
14 legal assistance request, U.S. authorities examined a mobile phone taken from one of the  
15 previously mentioned hacking group members while he was on vacation. The mobile  
16 phone contained communications with other members of the hacking group regarding the  
17 group's illegal activity, including Telegram, Threema, and Viber communications.

18 **B. Denys Iarmak**

19 29. U.S. authorities have identified multiple members of the hacking group,  
20 including DENYS IARMAK, also known as Denys Olegovich Iarmak, Denis Jarmak,  
21 and Denys Olehovych Yarmak, a resident and citizen of Ukrainian. Since at least 2016,  
22 IARMAK, who used online aliases such as "gaktus," "denis.jarmak", and "gaktus01"  
23 served as a hacker within the group and was involved in attacking multiple victim  
24 companies, including the successful hacks of several restaurant chains located in the  
25 United States.

26 30. As with other members of the hacking group, IARMAK used the virtual  
27 work environment to collaborate and coordinate with other group members. For instance,  
28 on July 24, 2017, IARMAK used Jabber to exchange stolen victim information with

1 another group member, Fedir Hladyr, charged in this District (*United States v. Hladyr*,  
2 CR17-276RSM). Furthermore, on March 3, 2017, IARMAK, using the alias “gaktus,”  
3 updated a JIRA issue he had created for a specific victim company and uploaded data he  
4 had stolen from that U.S. company. IARMAK had access to approximately 25 JIRA  
5 issues on Server-1 and 20 JIRA issues on Server-2.

6 31. In a Jabber conversation between IARMAK and Hladyr on October 20,  
7 2017, Hladyr provided user credentials for a compromised U.S. business. On October 27,  
8 2017, IARMAK replied back to Hladyr with internal system information of compromised  
9 machines related to the U.S. business. Through this investigation, authorities have  
10 confirmed that this hacking group stole payment card data from that U.S. business.

11 32. IARMAK frequently used the aliases “denis.jarmak” and “gaktus” when  
12 communicating with other members of the hacking group. For example, on December  
13 24, 2016, in a Jabber communication between Hladyr and IARMAK  
14 (denis.jarmak@jabber.ru), according to a machine translation, IARMAK told Hladyr to  
15 add him into a room and provided the name “GakTus.”

16 33. Like other members of the group, IARMAK provided his true name in  
17 order to receive payment for his work in furtherance of the group. For example, in a  
18 December 26, 2016 Jabber chat with one of the leaders of the hacking group, IARMAK  
19 (denis.jarmak@jabber.ru) sent his PrivateBank account number to receive salary  
20 payments. Further, through the investigation, authorities further identified IARMAK  
21 through his email account. For instance, authorities identified and later obtained a search  
22 warrant for IARMAK’s personal email account (denis.jarmak@gmail.com), which was  
23 linked to the PGP public key IARMAK used to have encrypted communications with  
24 other group members in furtherance of the coordinated hacking activities. According to  
25 records obtained from Google, the subscriber for this email account is Denis Jarmak.  
26 This email account contained photos of IARMAK’s Ukrainian passports and other  
27 identification documents. According to this and other documentation, [REDACTED]

28 [REDACTED] IARMAK is believed to




1 currently reside in Kyiv, Ukraine. The passport listed IARMAK's date of birth as  
2 XX/XX/1989. The email account also contained a copy of IARMAK's resume (which,  
3 according to a machine transliteration, was in the name Denys Olegovych Yarmak), with  
4 the same date of birth, and listed his father's, mother's, and sister's names, which was  
5 corroborated through other sources. IARMAK's resume listed work experience as a  
6 system administrator for multiple companies. The email account also contained a  
7 registration email for the aforementioned Jabber account (denis.jarmak@jabber.ru) and  
8 account creation and security alerts for one of IARMAK's linked email accounts,  
9 gaktus01@gmail.com, among others.

10 34. IARMAK also used the email account denis.jarmak@gmail.com in  
11 furtherance of the group's scheme. For example, in early April 2017, IARMAK  
12 exchanged multiple messages with an Anti-Virus (AV) company related to activating an  
13 AV product. IARMAK also forwarded copies of these emails to two other known members  
14 of the hacking group. Through the investigation, authorities have determined that one of  
15 the techniques used by the group is to check their various malware against AV products  
16 disconnected from Internet. This technique allows the group to determine whether the  
17 malware is being detected by the AV product as malicious without providing a copy of  
18 the malware to the AV companies.

19 35. In a translated Jabber communication on April 28, 2017, between  
20 IARMAK and Dmytro Fedorov, another known group member charged in this District  
21 (*United States v. Fedorov*, CR18-004RSM), IARMAK explained to Fedorov how to  
22 create the malware payload for a phishing document and referenced going into the  
23 machine with AV. IARMAK noted that a particular payload was detected by two AV  
24 companies, which meant that it was "burned somewhere." When Fedorov noted another  
25 tool used by the group that was tested against AV, IARMAK sought details on whether  
26 the testing was done with the interface to the Internet turned off. This conversation was  
27 consistent with the known methodology of the hacking group.  
28

1        36. In that same conversation, IARMAK also discussed phishing emails and  
2 specifically advised that he usually replaced the default picture of the embedded file  
3 which deploys malware if double clicked with some other image specific to the targeted  
4 company. As noted above, the investigation and security community reporting have  
5 observed that the phishing messages sent by this hacking group usually seek to  
6 manipulate targeted victims into double clicking on an image in the message attachment  
7 to activate malware and compromise machines on the victim network.

8        37. IARMAK also was implicated by other members of the hacking group. In  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18



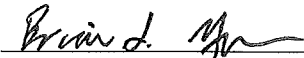
19 //

20 //

21 //

III. CONCLUSION

38. Based on the above facts, I respectfully submit that there is probable cause to believe that DENYS IARMAK did knowingly and intentionally committed the offenses of Conspiracy to Commit Computer Fraud and Abuse, in violation of Title 18, United States Code, Section 371, and Access Device Fraud, in violation of Title 18, United States Code, Sections 1029(a)(3), 1029(b)(1), 1029(c)(1)(A), and 2.

  
Briana L. Neumiller, Complainant  
Special Agent, Federal Bureau of  
Investigations

Based on the Complaint and Affidavit sworn to before me, and subscribed in my presence, the Court hereby finds that there is probable cause to believe the Defendant committed the offenses set forth in the Complaint.

Dated this 20<sup>th</sup> day of November, 2019.

  
MICHELLE L. PETERSON  
United States Magistrate Judge